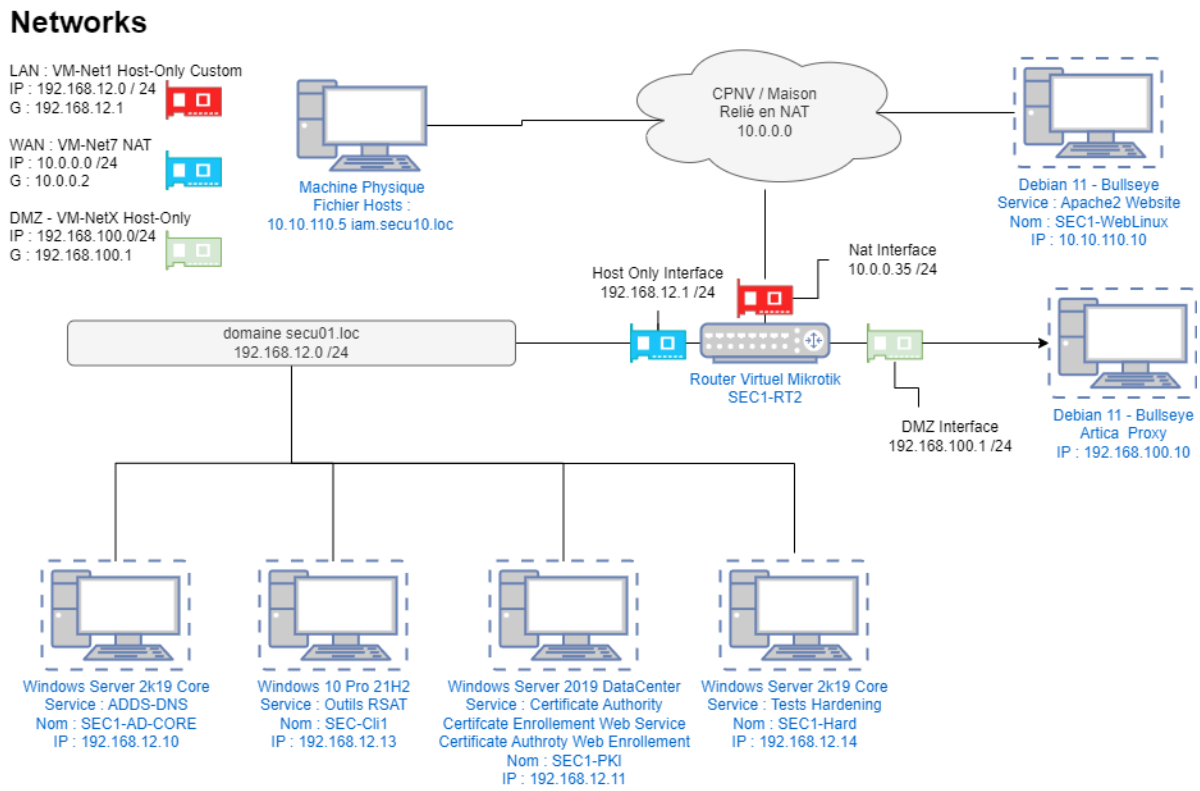
POC DMZ - Rapport de mise en service

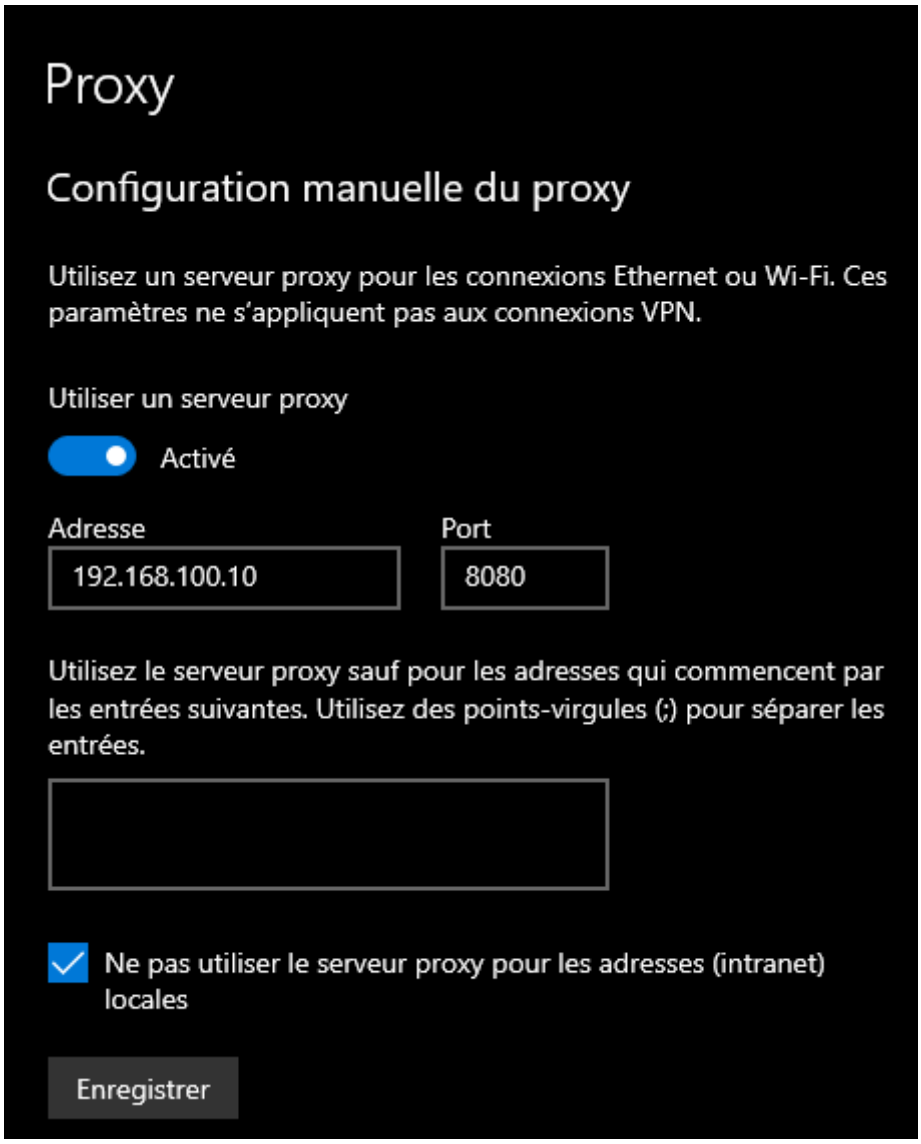
Table des matières

Schéma de l'infrastructure



User Story 1

```
En tant qu'utilisateur du LAN j'aimerai accéder à Internet de manière sécurisée
dans le but de ne pas compromettre la sécurité de mon entreprise.

- Copie d'écran de la config du proxy dans le navigateur
```

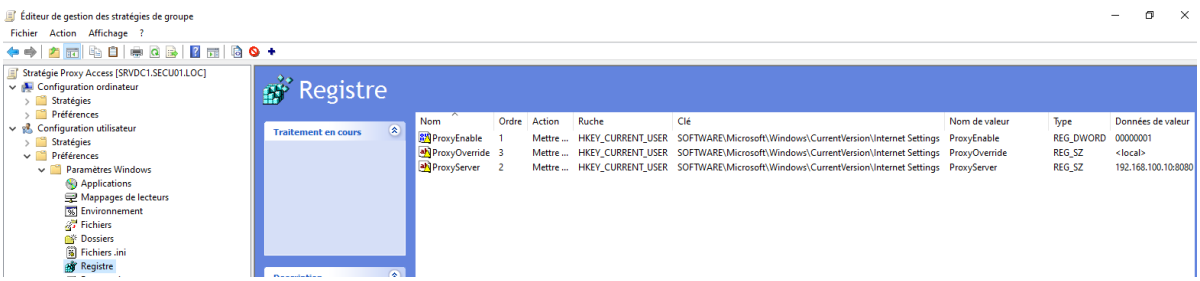


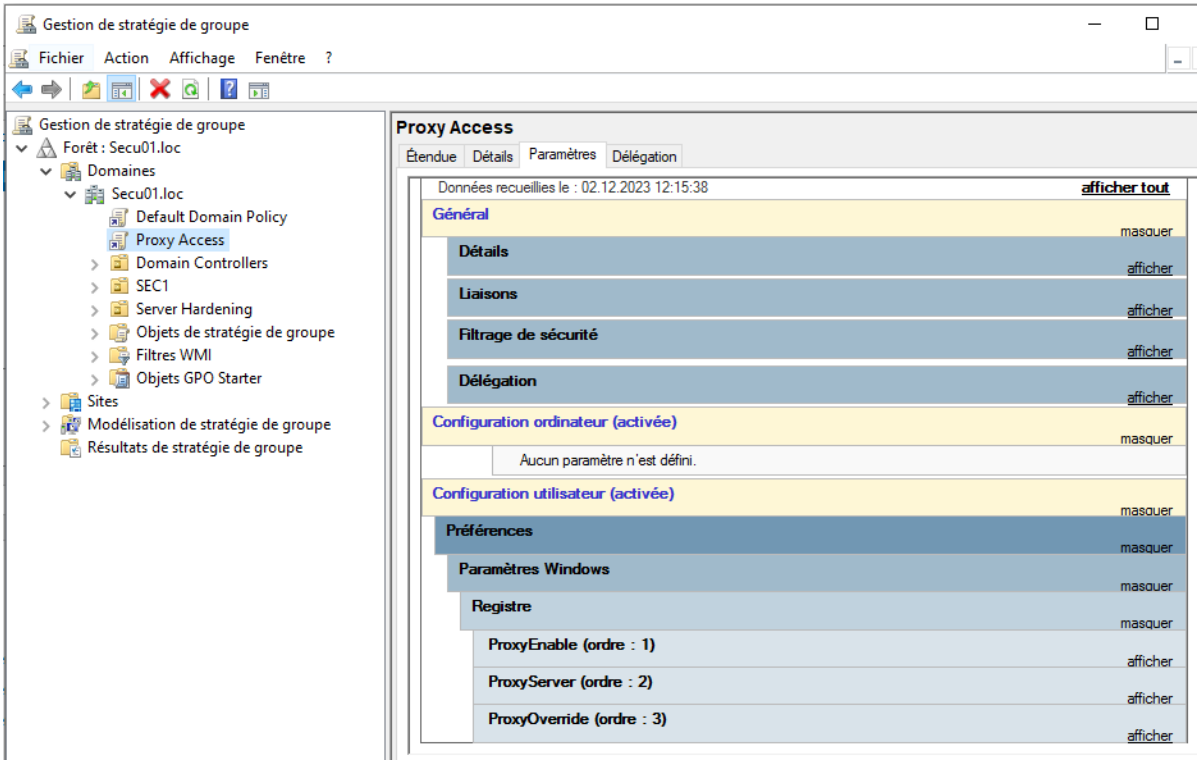
User Story 2

En tant qu'utilisateur du LAN j'aimerai que mon navigateur soit configuré de manière automatique au niveau du proxy à utiliser, dans le but de se simplifier la vie.

- Copie d'écran de la GPO, proxy.pac ou autre config

- <local> dans overide modifié par "192.168.12.*" *lors de la config de radius*





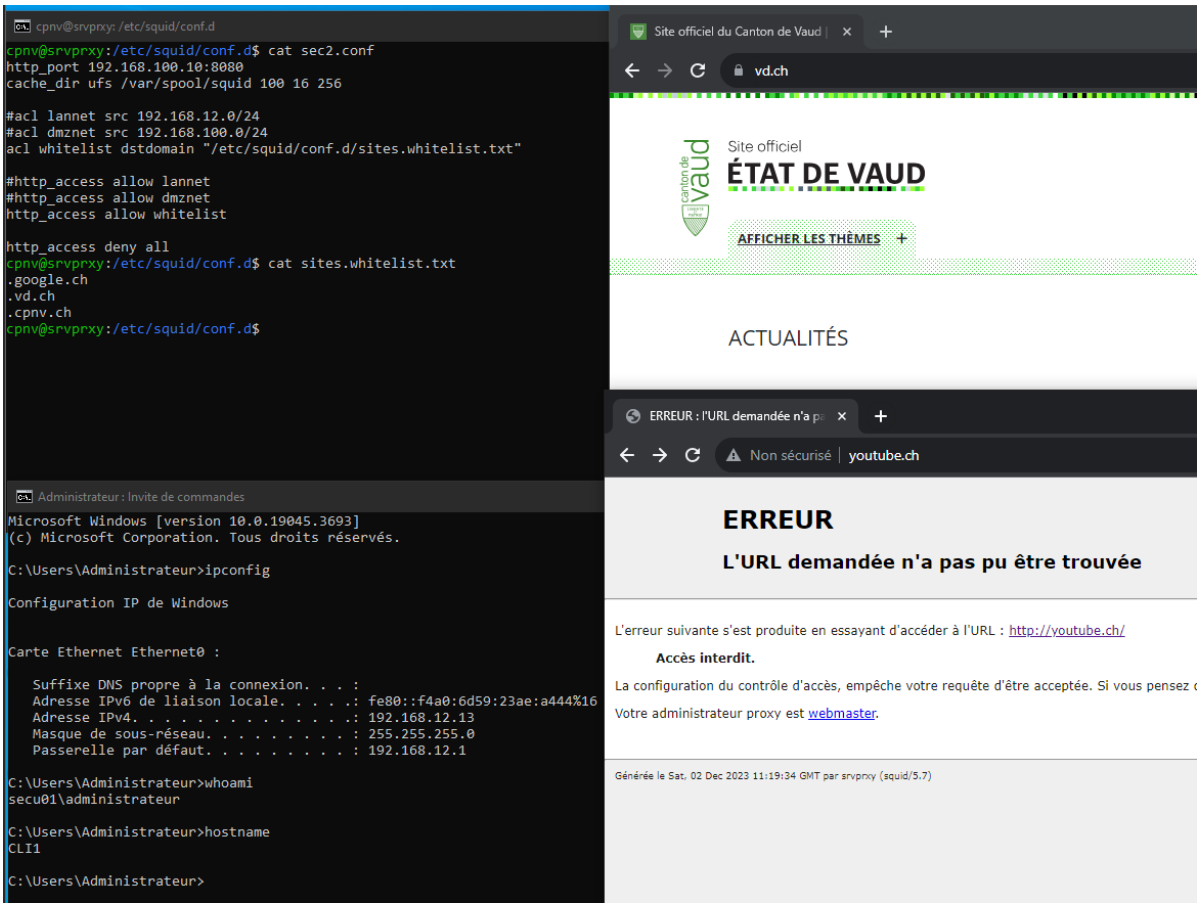
User Story 3

```
En tant que responsable de la sécurité, j'aimerai que les machines de mon
infrastructure
puissent communiquer en respectant les principes d'une DMZ, dans le but de
sécurisé
mon infrastructure contre la compromission d'une ou plusieurs machines.

- Tableau des règles du firewall
```

Source	Destination	Protocol	Action
LAN	Any	Any	Block
LAN	DMZ	8080 (SquidProxy)	Pass
DMZ	WAN	443 (HTTPS)	Pass
DMZ	LAN (192.168.12.11)	1812 (RADIUS)	Pass
WAN	DMZ (192.168.100.10)	80 (HTTP)	Pass

User Story 4

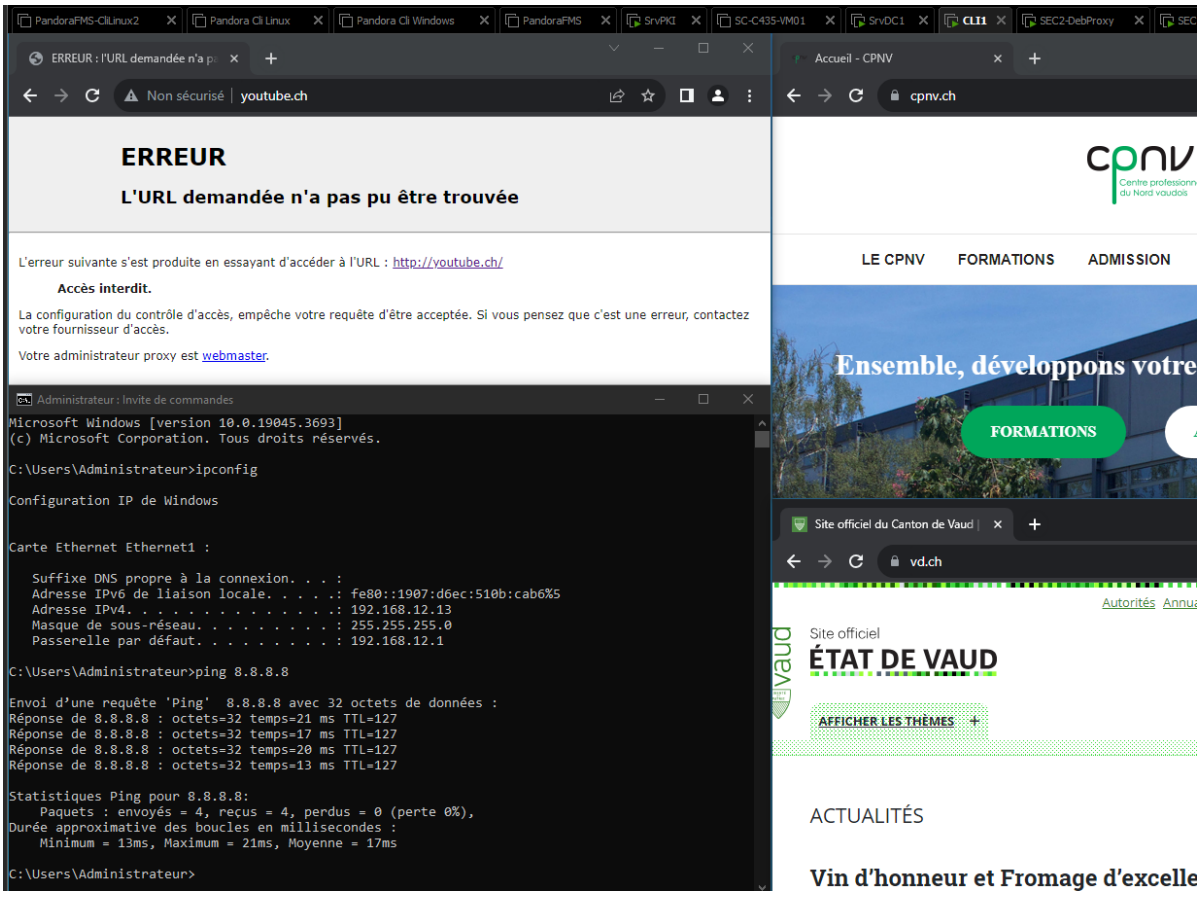
```
En tant que CTO, j'aimerai que les utilisateurs du LAN puissent surfer sur un
nombre
restreint de sites (www.cpnv.ch, www.vd.ch), pour améliorer leur productivité.

- Caputre d'écrans : config squid et test accès depuis le Cli1 à vd.ch et youtube

- Parfois la page d'erreur squid s'affiche parfois non et c'est juste une page
d'erreur google
```



User Story 5

En tant que responsable de la sécurité, j'aimerai que le LAN puisse accéder au WAN uniquement à l'aide de ping et protocoles web (https, http), dans le but de protéger l'infrastructure

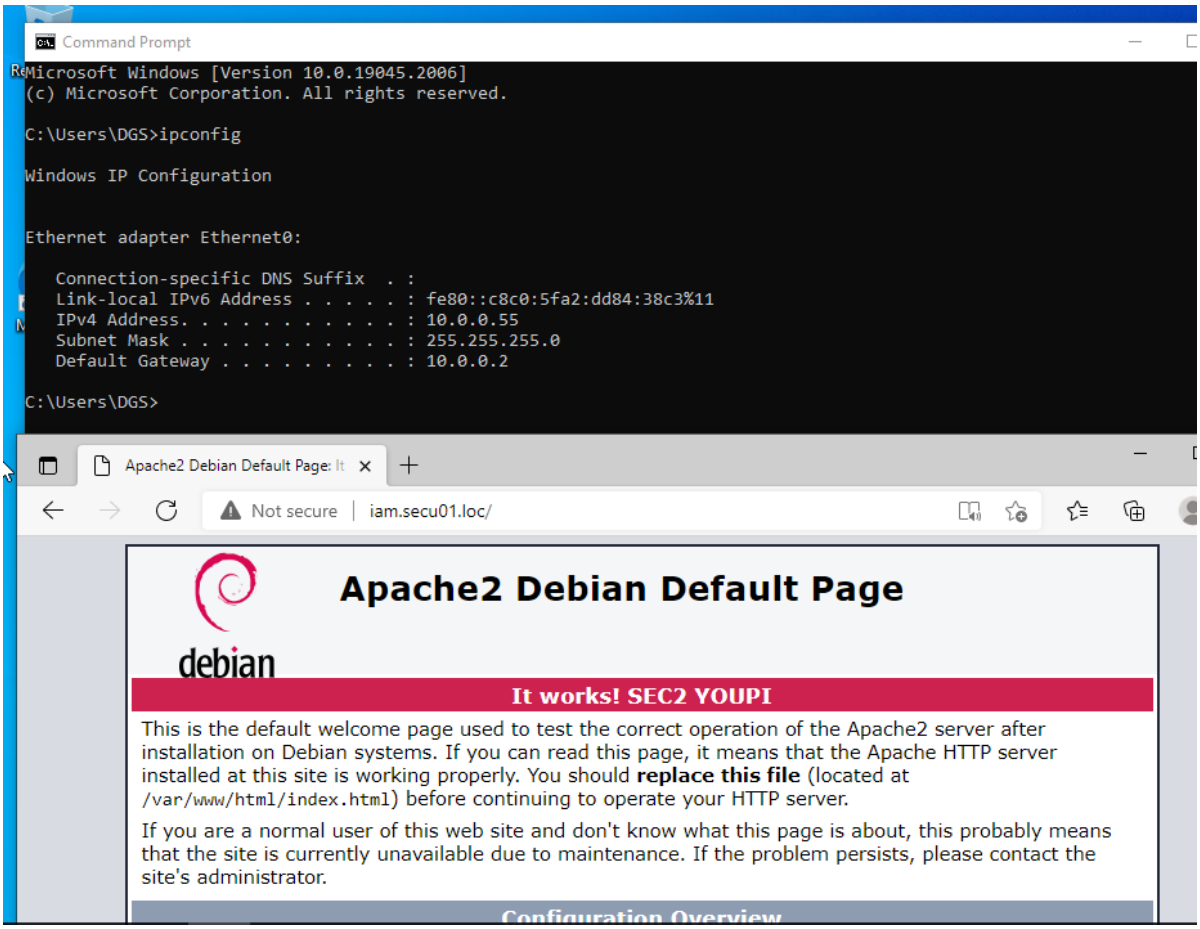
- Accès only au ping, ping 8.8.8.8 passe mais sur le web only vd.ch
- Depuis CLI1, ping 8.8.8.8 ok avec accès au sites voulus mais pas aux autres



User Story 6

En tant que responsable informatique, je veux que les internautes puissent avoir accès à un site web dans le DMZ qui réponde à http://iam.secuxx.internal, dans le but de par la suite mettre en place un service d'authentification.

- Machine ajoutée - Client Windows dans le NAT, problème avec opnsense pour sortir sur pc physique, accèes et règles OK pour WAN mais pas pour pc physique


Command Prompt
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
C:\Users\DGS>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::c8c0:5fa2:dd84:38c3%11
IPv4 Address. . . . . : 10.0.0.55
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.0.2
C:\Users\DGS>
Apache2 Debian Default Page: It
Not secure
iam.secu01.loc/
Apache2 Debian Default Page
debian
It works! SEC2 YOUPI
This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should replace this file (located at /var/www/html/index.html) before continuing to operate your HTTP server.
If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.
Configuration Overview